附件：

医养信息系统安全等级保护测评服务项目

需求书

一、测评内容

测评机构应根据等保测评的相关文件要求，按照我单位的需求完成对网络安全等级保护状况测试评估工作，应做到两个方面的内容：一是安全控制测评，主要测评网络安全等级保护要求的基本安全控制在信息系统中的实施配置情况；二是系统整体测评，主要测评分析信息系统的整体安全性。其中，安全控制测评是信息系统整体等级保护测评的基础。

**（一）安全控制测评**

测评机构应按照要求完成安全控制测评，安全控制测评可分为安全技术测评和安全管理测评两大类。安全技术测评包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个层面的安全控制测评；安全管理测评包括：安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全系统运维五个方面的安全控制测评。

1.安全物理环境

测评机构可通过访谈、文档审查和实地察看的方式测评信息系统的物理安全保障情况。主要涉及对象为机房及相关配套设施。

2.安全通信网络

测评机构可通过访谈、配置检查和工具测试的方式测评信息系统的网络安全保障情况。主要涉及对象为网络互联设备、网络安全设备和网络拓扑结构等三大类对象。

3.安全区域边界

测评机构可将通过访谈、配置检查和工具测试的方式测评信息系统的网络边界安全保障情况。重点测评的包括各边界防火墙，交换机等。

4.安全计算环境

测评机构应按照我方的要求通过访谈、配置检查和工具测试的方式测评信息系统的操作系统、数据库等保障情况。

5.安全管理中心

测评机构可通过访谈、配置检查的方式测评信息系统的安全管理中心保障情况，主要涉及对象为纳入测评范围的安全管理中心等。

6.安全管理部分

安全管理部分为全局性问题，按照信息等级保护的有关要求，应对至少包括安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全系统运维等五个方面的安全控制测评。

**（二）系统整体测评**

测评机构测评人员应根据服务对象涉及系统具体情况，结合《网络安全等级保护测评准则》要求，确定系统整体测评的具体内容，至少包括四个部分：安全控制间安全、层面间安全、区域间安全、系统结构安全进行测评。

1.安全控制间等级保护测评

安全控制间的等级保护测评主要为同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。安全功能上的增强和补充可以使两个不同强度、不同等级的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。例如，可以通过物理层面上的物理访问控制来增强其安全防盗窃功能等。安全功能上的削弱会使一个安全控制的引入影响另一个安全控制的功能发挥或者给其带来新的脆弱性。例如，应用安全层面的代码安全与访问控制，如果代码安全没有做好，很可能会使应用系统的访问控制被旁路。

2.层面间等级保护测评

层面间的等级保护测评主要为同一区域内的不同层面之间存在的功能增强、补充和削弱等关联作用。安全功能上的增强和补充可以使两个不同层面上的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。安全功能上的削弱会使一个层面上的安全控制影响另一个层面安全控制的功能发挥或者给其带来新的脆弱性。

3.区域间等级保护测评

区域间的等级保护测评主要为互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。例如，流入某个区域的所有网络数据都已经在另一个区域上做过网络安全审计，则可以认为该区域通过区域互连后具备网络安全审计功能。安全功能上的增强和补充可以使两个不同区域上的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。安全功能上的削弱会使一个区域上的安全功能影响另一个区域安全功能的发挥或者给其带来新的脆弱性。

4.系统结构等级保护测评

系统结构等级保护测评主要为信息系统整体结构的安全性和整体安全防范的合理性。例如，由于信息系统边界上的网络入侵防范设备的管理接口连接方式不当，可能使网络访问控制出现旁路，出现信息系统整体安全防范不当。测评分析信息系统整体结构的安全性，主要是指从信息安全的角度，分析信息系统的物理布局、网络结构和业务逻辑等在整体结构上是否合理、简单、安全有效。测评信息系统整体安全防范的合理性，主要是指从系统的角度，分析研究信息系统安全防范在整体上是否遵循纵深防御的思路，明晰系统边界，确定重点保护对象，在适当的位置部署恰当的安全技术和安全管理措施等。

二、测评对象与计划

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **系统名称** | **计划达到**  **安全等级** | **备案情况** |
| 1 | 网站系统 | 二级 | 未备案 |
| 2 | HIS和PACS系统 | 二级 | 未备案 |
| 3 | 检验信息系统 | 二级 | 未备案 |
| 4 | 养老信息系统 | 二级 | 未备案 |
| 5 | 体检信息系统 | 二级 | 未备案 |

三、服务要求

|  |  |
| --- | --- |
| 定级  备案 | 按照《网络安全等级保护定级指南》以及《网络安全等级保护管理办法》等文件的要求，协助我单位完成信息系统安全等级保护定级备案材料编制工作并出具《专家评审意见表》，并提交给公安部门协助申请办理备案证。 |
| 差距  测评 | 根据被测系统安全等级保护定级情况，制定信息系统安全等级保护测评方案，对信息系统涉及的机房、网络/安全设备、主机设备、应用系统、安全管理体系等进行等级保护差距测评，并提交不符合项表和整改建议。出具《网络安全等级保护测评问题单》 |
| 漏洞  扫描 | 对被测信息系统服务器、应用系统进行漏洞扫描，列出被测信息系统中存在的主要问题以及可能造成的后果，并提出整改建议。 |
| 渗透  测试 | 根据扫描结果进行漏洞分析及说明，对二级互联网信息系统开展渗透测试，进行弱口令测试及其他手工测试，并提交修复建议。 |
| 回归  测评 | 用户完成整改工作后，依据《GBT28448-2019信息安全技术网络安全等级保护测评要求》及相关等保2.0标准和要求，对信息系统进行验收性测评（现场测评），并出具《网络安全等级保护测评报告》。 |

四、成果文件

项目的实施提交成果文件包括但不限于：

1.《广东省社会福利服务中心（广东江南医院）单位信息系统安全等级保护定级备案资料》

2.《广东省社会福利服务中心（广东江南医院）单位信息系统安全等级保护差距测评问题清单》

3.《广东省社会福利服务中心（广东江南医院）单位信息系统安全等级保护回归测评报告》